IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 2136
Christopher E. Barnabo et al.	:	Examiner: David Garcia Cervetti
Serial No.: 10/600,215	:	IBM Corporation
Filed: 06/20/2003	:	Intellectual Property Law
Title: SYSTEM AND METHOD FOR AUTHENTICATION TO AN APPLICATION	:	Department SHCB/040-3
	:	1701 North Street
	:	Endicott, NY 13760
Confirmation No.: 5835		

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

I. Real Party in Interest

International Business Machines Corporation is the real party in interest.

II. Related Appeals and Interferences

There are no related appeals or interferences.

III. Status of Claims

Claims 1-7, 11-14 and 16-26 are pending, Finally Rejected and Appealed.

Claims 8-10 and 15 were previously canceled.

IV. Status of Amendments

An Amendment After Final Action was electronically filed on 07/20/07 to correct a reference number and supply another, missing reference number in Figure 1. This Amendment has been entered.

V. Summary of Claimed Subject Matter

Support for the claim elements is indicated in plain brackets [ ].

Claims 1, 16 and 21 recite a method, system and program product for authenticating a first user [user 25 of Figure 1] in a protected network [Blue Zone network 12] to an application [Application 30 of Figure 1 and Page 5 lines 8-13 and 16-21] shared concurrently with a second user [User 53 in Figure 1 in Red Zone network 16. Page 8 lines 25-26] in an unprotected network. [Red Zone network 16 or Internet 54] The first user [User 25 in Blue Zone 12] supplies a userID and a password to a first server [Server 20] within the protected network for authentication for the application. [Steps 100-105 of Figure 3A and Page 6 line 22 to Page 7 line 4.] The application [Application 30] resides in a third network [Yellow Zone network 14] configured as a buffer between the protected network [Blue Zone network 12] and the unprotected network [Red Zone network 16]. The user's password is not sent from the protected network into the third network to access the application. [Page 7 lines 9-18.] The first server determines that the userID and password are authentic. [Step 104 and Decision 105, yes branch and Page 7 lines 1-4.] In response, the first server [Server 20] forwards to the application [Application 30] an authentication key for the first user and a selection by the first user pertaining to the application. [Step 110 and Page 7 lines 9-26.] The application determines that the key is authentic. [Step 114 and 116 and Page 7 line 26 to Page 8 line 4.] In response, the application complies with the selection by the first user. [Step 124 and Page 8 lines 3-7.] The second user [User 53 in Red zone] supplies another userID and another password to the application. [Steps 300, 302 and 304 of Figure 4A and Page 8 line 25 to Page 9 line 1.] The application determines that the other userID [for User 53 in Red Zone] and the other password

are authentic [Step 306 and Decision 308, yes branch and Page 9 lines 1-4], and in response, the application complies with a selection made by the second user pertaining to the application. [Step 316 and Page 9 lines 3-5.]

Claim 14 depends on claim 1 and recites that the authentication key is self authenticating based on whether a period during which the key is valid matches a scheduled period of use of the application, and whether an IP address of the first user is from the protected network [Page 7 line 23 to Page 8 line 1.]

Structure, material or acts corresponding to each means plus function element are indicated in stylized brackets { }.

16. An authentication system comprising:

an application [Application 30, Page 5 lines 8-13 and 16-21, and equivalents] on a first server [Server 40, and equivalents] in a first network [Yellow Zone or buffer network 14, and equivalents];

a second server {Server 20 and equivalents} in a second, protected network {Blue Zone 12 or Intranet 22 and equivalents and equivalents} to receive from a first user {user 25, and equivalents} within said second network a userID and a password for authentication for said application, said second server including means for checking authentication of said first user based on said userID and password {Step 104 and Decision 105 of Figure 3A and Page 7 lines 1-4, and equivalents.}, and if said first user is authentic, forwarding to said application an authentication key for said first user and a selection by said first user pertaining to said application {Step 110 and Page 7 lines 9-13, and equivalents.}, said password not being sent from said protected network into said first network to access said application; and

said application including means for checking authentication of said key {Step 114 and 116 and Page 7 lines 13-14 or Page 7 line 23 to Page 8 line 1, and equivalents.}, and if authentic,

complying with said selection by said first user {Step 124 and Page 8 lines 3-5, and equivalents.}; and

a workstation in a third, unprotected network {Red Zone 16 or Internet 54, and equivalents} for a second user {User 53 in Red Zone 16 or Internet 54, and equivalents}, said application being shared concurrently with said first and second users, said first network configured as a buffer between said second, protected network and said third, unprotected network; and wherein

said application receives from said second user another userID and another password, and includes means for determining that said other userID and other password are authentic {Step 306 and Decision 308, yes branch and Page 9 lines 1-5, and equivalents}, and in response, complying with a selection made by said second user pertaining to said application {Step 316 and Page 9 lines 3-5, and equivalents}.

VI. Grounds of Rejection to be reviewed on Appeal

Claims 1-3, 7, 11-13, 16-18 and 21-25 were rejected under 35 USC 102 based on US Patent 7,197,751 to Fedotov et al.

Claims 4-6, 19, 20 and 26 were rejected under 35 USC 103 based on Fedotov et al. in view of "NPL Oracle iMeeting" by Roy et al.

Claim 14 was rejected under 35 USC 103 based on Fedotov et al and US Patent 7,111,323 to Bhatia et al.

(All three of these references were newly cited in the Final Rejection.)

VII. Argument

A claim can be rejected under 35 USC 102 only if each and every element as recited in the claim is found in a single prior art reference. Richardson v. Suzuki Motor Co., 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

A claim cannot be obvious under 35 USC 103 unless (a) there is a reason that a person of ordinary skill in the art would have combined the references, and (b) all the claim elements are taught or suggested by the prior art. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438, 1443 (Fed Cir. 1991) and KSR Int'l Co. v. Teleflex, Inc., No. 04-1350 (USSC 30 April 2007).

Rejection of Claims 1, 11-13, 16 and 21-22 under 35 USC 102
Based on Fedotov et al.

Claim 1 recites a method, system and program product for authenticating a first user in a protected network to an application shared concurrently with a second user in an unprotected network. The first user supplies a userID and a password to a first server within the protected network for authentication for the application. The application resides in a third network configured as a buffer between the protected network and the unprotected network. The user's password is not sent from the protected network into the third network to access the application. The first server determines that the userID and password are authentic. In response, the first server forwards to the application an authentication key for the first user and a selection by the first user pertaining to the application. The application determines that the key is authentic. In response, the application complies with the selection by the first user. The second user supplies another userID and another password to the application. The application determines that the other userID and the other password are authentic, and in response, the application complies with a selection made by the second user pertaining to the application.

Thus, according to claim 1, the first user in a protected network authenticates himself or herself to a first server in the protected network, and the first server in the protected network forwards to an application in a buffer network an authentication key for the first user. Consequently, the password of the first user need not be and is not sent into the buffer network to access the application. Therefore, the user's password cannot be discovered by a hacker with access to the application in the buffer network. Also according to claim 1, a second user in an unprotected network sends his or her userID and password to the application in the buffer network for authentication. Thus, the application in the buffer network supports authentication in two different manners (with the aid of the first server in the protected network). In contrast to claim 1, Fedotov et al. disclose a single network 104 which interconnects all clients 102a-m to a collaboration server 110. The "collaboration server" includes a web server 112, MX modules 114a-n and Organizers 116. See Figure 1 of Fedotov et al.. As illustrated in Figure 1 of Fedotov et al., all clients 102a-m of Fedotov et al. access collaboration server 110 via the same network 104. Also, all clients 102a-m authenticate themselves **directly** to the web server 112 in the

collaboration server 110. In contrast to claim 1, in Fedotov et al. there is no two step authentication of a user in a protected network to an application in a buffer network via an intermediary server in the protected network. Also, Fedotov et al. presumably support only one manner of authentication for all clients to collaboration server 110:

> "Figure 5 demonstrates a method of connecting a new attendee to a collaboration session, according to one embodiment of the invention. In state 502, a new attendee connects to a collaboration web server, through his or her client computing device (e.g. with a suitable browser). A listener in the web server accepts and forwards the connection to an available MX module. A communication layer of the organizer managing the target collaboration establishes or accepts a virtual channel between the organizer and the client.
>
> In state 504, after the new client is authenticated, a unique client ID is assigned to the client." Fedotov et al. Column 14 lines 34-50.

Thus, Fedotov et al. teach a substantially different architecture than claim 1 of the present invention which involves three different networks - a protected network with an authentication server and key manager, a buffer network and an unprotected network. Fedotov et al. teach a substantially different authentication and client request management process than claim 1. According to claim 1, a user at the protected network authenticates himself or herself to a server in the protected network and furnishes a request for the application in the buffer network, and the server **in the protected network** uses a key to authenticate to the application in the buffer network. Next, the application processes the client request. Another user in the unprotected network passes his or her userID and password to the application in the buffer network. A password of the person **at the protected network** is not sent to the buffer network to access the application. This prevents a hacker at the unprotected network with access to the application in the buffer network from learning the password of the user at the protected network from the buffer network. In contrast to claim 1, Fedotov et al. disclose only one manner of authentication for all clients and this involves forwarding the userID and password through the same network 104 to the collaboration server 110. Also, Fedotov et al. disclose only one manner of forwarding client requests to the collaboration server 110, and this does not involve an intermediary server

in a protected network. Therefore, the rejection of claim 1 under 35 USC 102 based on Fedotov et al. should be reversed. Moreover, Fedotov et al. make no suggestion of the foregoing architecture of claim 1 including a protected network with an authentication server and key manager, buffer network and unprotected network or the two step manners of authentication of clients and forwarding of client requests to the application. Therefore, no rejection under 35 USC 103 should be made to claim 1.

Claims 11-13 depend on claim 1, and therefore distinguish over the prior art for the same reasons as claim 1. Therefore, the rejection of claims 11-13 under 35 USC 102 based on Fedotov et al. should be reversed, and no rejection under 35 USC 103 should be made.

Independent claim 16 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. Therefore, the rejection of claim 16 under 35 USC 102 based on Fedotov et al. should be reversed, and no rejection under 35 USC 103 should be made.

Independent claim 21 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. Therefore, the rejection of claim 21 under 35 USC 102 based on Fedotov et al. should be reversed, and no rejection under 35 USC 103 should be made.

Rejection of Claims 2, 17 and 22 under 35 USC 102
Based on Fedotov et al.

Claim 2 depends on claim 1 and recites that the application complies with the selection made by said second user without the second user supplying an authentication key to the third network. This confirms that the server in the protected network provides the authentication to the application in the buffer network needed for the application in the buffer network to comply with the request of the user in the protected network. As explained above, Fedotov et al. do not teach or suggest that a user in the protected network authenticates himself or herself to a server in the protected network and furnishes a request to the server in the protected network for the application in the buffer network, and the server in the protected network uses a key to authenticate to the application in the buffer network. After authentication, the application in the

buffer network processes the client request. Claim 2 also distinguishes over Fedotov et al. for the same reasons that base claim 1 distinguishes thereover. Therefore, the rejection of claim 2 under 35 USC 102 should be reversed, and no rejection under 35 USC 103 should be made.

Claim 17 depends on Claim 16 and distinguishes over Fedotov et al. for the same reasons that claim 2 (and claim 16) distinguishes thereover. Therefore, the rejection of claim 17 under 35 USC 102 should be reversed, and no rejection under 35 USC 103 should be made.

Claim 22 depends on Claim 21 and distinguishes over Fedotov et al. for the same reasons that claim 2 (and claim 21) distinguishes thereover. Therefore, the rejection of claim 22 under 35 USC 102 should be reversed, and no rejection under 35 USC 103 should be made.

Rejection of Claims 3 and 18 under 35 USC 102
Based on Fedotov et al.

Claim 3 depends on claim 1 and recites that the protected network and the third network are both controlled by a same entity. This provides a measure of security to the third, buffer network relative to the protected network. As explained above, Fedotov et al. do not teach or suggest that a user in the protected network authenticates himself or herself to a server in the protected network and furnishes to the server in the protected network a request for the application in the buffer network (where the buffer network is controlled by a same entity as controls the protected network), and the server in the protected network uses a key to authenticate to the application in the buffer network. Next, the application in the buffer network processes the client request. Claim 3 also distinguishes over Fedotov et al. for the same reasons that base claim 1 distinguishes thereover. Therefore, the rejection of claim 3 under 35 USC 102 should be reversed, and no rejection under 35 USC 103 should be made.

Claim 18 depends on Claim 16 and distinguishes over Fedotov et al. for the same reasons that claim 3 (and claim 16) distinguishes thereover. Therefore, the rejection of claim 18 under 35 USC 102 should be reversed, and no rejection under 35 USC 103 should be made.

Rejection of Claim 7 under 35 USC 102
Based on Fedotov et al.

Claim 7 depends on claim 1 and recites that the selection by the first user is a "request" to the application, and the selection by the second user is a request to the application. This confirms that the first user at the protected network makes a request to the server in the protected network for the application in the buffer network, and after the server in the protected network authenticates to the application in the buffer network based on a key, the application in the buffer network processes the client request. This is not taught or suggested by Fedotov et al. Therefore, the rejection of claim 7 based on 35 USC 102 should be reversed, and no rejection under 35 USC 102 should be made.

Rejection of Claim 23 under 35 USC 102
Based on Fedotov et al.

Independent claim 23 recites a method for authenticating a first user of a first computer in a protected network to a second computer executing an application. A second user of a third computer in an unprotected network and the first user of the first computer concurrently share the application. The second computer resides in a third network configured as a buffer between the protected network and the unprotected network. The first computer supplies a userID and a password of the first user to a fourth computer in the protected network for authentication for the application. The fourth computer determines that the userID and password are authentic. In response, the fourth computer forwards to the second computer an authentication key for the first user. The password is not sent from the protected network into the third network to access the application. The second computer determines that the key is authentic, and in response, complies with a selection by the first user pertaining to the application. The third computer supplies another userID and another password of the second user to the second computer. The second computer determines that the other userID and the other password are authentic. In response, the application complies with a selection made by the second user pertaining to the application.

Independent claim 23 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover, except that claim 23 does not recite that the computer in the protected network forwards a selection of the client in the protected network to the application in the buffer network.

Thus, according to claim 23, the first user in a protected network authenticates himself or herself to a fourth computer in the protected network, and the fourth computer in the protected network forwards to an application in a buffer network an authentication key for the first user. Consequently, the password of the first user need not be and is not sent into the buffer network to access the application. Therefore, the user's password cannot be discovered by a hacker with access to the application in the buffer network. Also according to claim 23, a second user in an unprotected network sends his or her userID and password to the application in the buffer network for authentication. Thus, the application in the buffer network supports authentication in two different manners (with the aid of the fourth computer in the protected network). In contrast to claim 1, Fedotov et al. disclose a single network 104 which interconnects all clients 102a-m to a collaboration server 110. The "collaboration server" includes a web server 112, MX modules 114a-n and Organizers 116. See Figure 1 of Fedotov et al. As illustrated in Figure 1 of Fedotov et al., all clients 102a-m of Fedotov et al. access collaboration server 110 via the same network 104. Also, all clients 102a-m authenticate themselves directly to the web server 112 in the collaboration server 110. In contrast to claim 23, Fedotov et al. do not teach or suggest a two step authentication to an application in a buffer network via an intermediary server in a protected network or more than one manner of authentication to collaboration server 110. Fedotov et al. do not teach or suggest three different networks - a protected network with an authentication server, a buffer network and an unprotected network. Fedotov et al. do not teach or suggest that a user in the protected network authenticates himself or herself to a server in the protected network, and the server **in the protected network** uses a key to authenticate to the application in the buffer network. Fedotov do not teach or suggest that a password of a person **in a protected network** is not sent to a buffer network to access the application to prevent a hacker in an unprotected network with access to the application in the buffer network from learning the password from the buffer network. In contrast to claim 23, Fedotov et al. disclose only one manner of authentication for all clients and this involves forwarding the userID and password

through the same network 104 to the collaboration server 110. Fedotov et al. disclose only one manner of forwarding client requests to the collaboration server 110, and this does not involve an intermediary server in a protected network. Therefore, the rejection of claim 23 under 35 USC 102 based on Fedotov et al. should be withdrawn. Moreover, Fedotov et al. make no suggestion of the foregoing architecture of claim 23 including a protected network with an authentication server, buffer network and unprotected network or the two step authentication process. Therefore, no rejection under 35 USC 103 should be made to claim 23.

Rejection of Claim 24 under 35 USC 102
Based on Fedotov et al.

Claim 24 depends on Claim 23 and distinguishes over Fedotov et al. for the same reasons that claim 2 (and claim 23) distinguishes thereover. Therefore, the rejection of claim 24 under 35 USC 102 should be reversed, and no rejection under 35 USC 103 should be made.

Rejection of Claim 25 under 35 USC 102
Based on Fedotov et al.

Claim 25 depends on Claim 23 and distinguishes over Fedotov et al. for the same reasons that claim 3 (and claim 23) distinguishes thereover. Therefore, the rejection of claim 25 under 35 USC 102 should be reversed, and no rejection under 35 USC 103 should be made.

Rejection of Claims 4, 19 and 26 under 35 USC 103
Based on Fedotov et al. in view of Roy et al.

Claims 4, 19 and 26 specify that the buffer network acts as a "security" buffer for the protected network. As noted above, Fedotov et al. Fedotov et al. do not teach or suggest authentication of a user at a protected network to a server in the protected network and authentication of the server in the protected network to an application in the buffer network with a key to allow a user request from the protected network to be processed by the application in the buffer network. Fedotov et al. do not teach or suggest that a password of a person at the protected network is not sent to a buffer network to access the application to prevent a hacker in an unprotected network with access to the application in the buffer network from learning the password from the buffer network. Fedotov et al. do not teach the security buffer network of claims 4, 19 and 26.

Roy et al. disclose that an iMeeting system can be deployed in a DMZ "where attendees from the Internet (outside the company firewall) as well as attendees from the Intranet (inside the company firewall) participate in the same iMeeting session. ... The iMeeting System is located in a DMZ while the database server and the Document Conversion server are located inside the firewall in the Intranet." Roy et al. Page 1-7 Section 1.2.3. Roy et al. also teach a **direct/one step** authentication by users to an iMeeting session: "Logging into iMeeting. Log into iMeeting using a user account that has the iMeeting End User responsibility." Roy et al. Page 2-14 Section 2.7. Thus, Roy et al. do not teach or suggest a two step authentication, i.e. authentication of a user in a protected network to a server in a protected network and authentication of the server in the protected network to an application in a buffer network. Roy et al. do not teach or suggest that the server in the protected network passes the key to the application in the buffer network. Roy et al. do not teach or suggest that a password of a person in a protected network is not sent to a buffer network to access the application to prevent a hacker in an unprotected network with access to the application in the buffer network from learning the password from the buffer network. Therefore, the rejection of claims 4, 19 an 23 under 35 USC 103 based on Fedotov et al. and Roy et al. should be reversed.

Rejection of Claims 5-6 and 20 under 35 USC 103
Based on Fedotov et al. in view of Roy et al.

Claims 5-6 and 20 depend on claims 1 and 16 respectively, and recite that the unprotected network is the Internet. This confirms the risk of allowing a userID and password of a person in a protected network to be sent to a buffer network. The present invention avoided this risk indicating a long felt need. This confirms the nonobviousness of the present invention as recited in claims 5-6 and 20. Claims 5-6 and 20 also distinguish over the Fedotov et al. for the same reasons that claims 1 and 16 distinguish thereover.

Rejection of Claim 14 under 35 USC 103
Based on Fedotov et al and Bhatia et al.

Claim 14 depends on claim 1 and recites that the authentication key is self authenticating based on whether a period during which the key is valid matches a scheduled period of use of the application, and whether an IP address of the first user is from the protected network. The Examiner acknowledges that Fedotov et al. do not teach this feature of claim 14, but asserts that Bhatia et al. fill this gap. In the Background section, Bhatia et al. disclose "a single sign-on environment allows a user access to 'partner' applications across the distributed computing environment after authenticating once with a single sign-on server." Bhatia et al. column 1 lines 32-35. Bhatia et al. also disclose "the system also determines if the authentication has expired because of nonuse for a specified period. This authentication is stored within a time-stamped token on the user device. If the authentication has not been received or has expired, the system redirects the access request to a single sign-on server for the distributed computing environment so that the user can reauthenticate with the distributed computing environment." Bhatia et al. Column 1 line 68 to Column 2 line 8. The flow chart of Figure 5 of Bhatia et al. also illustrates the steps of "User accesses an application", "Attempt to recover token", "Does user have token?", "Calculate expiry time", "Has token expired", If the token has not expired, "return token with updated time" and "Grant Access to the Application", If the token has expired, "redirect user to single signon server", "Request signon credentials" and "Validate sign-on

credentials". Figure 1 of Bhatia et al. illustrate a user device 102 which is coupled to a series of application servers 106, 108, 110 and 112 and a Single Sign-on server 114 via a network such as the Internet. Bhatia et al. also disclose that "Application servers 106, 108, 110 and 112 and single sign-on server 114 can use private network 116, if provided, for private communications (e.g. for sharing a common time among the various servers." However, Bhatia et al. do not teach or suggest authentication of a user in a protected network to a server in a protected network and authentication of the server in the protected network with a key to an application in a buffer network. Bhatia et al. do not teach or suggest three different networks - a protected network with an authentication server, a buffer network and an unprotected network. Bhatia et al. do not teach or suggest that the server in the protected network passes the key to the application in the buffer network. Bhatia et al. do not teach or suggest that a password of a person in a protected network is not sent to a buffer network to access the application to prevent a hacker in an unprotected network with access to the application in the buffer network from learning the password from the buffer network. Moreover, Bhatia et al. do not teach or suggest that the authentication key is self authenticating based on whether a period during which the key is valid matches a **scheduled period of use of the application**, **and whether an IP address of the first user is from the protected network.** Therefore, the rejection under 35 USC 103 should be reversed.

Based on the foregoing, all rejections of the present patent application should be reversed.

Respectfully submitted,

Dated: 07/31/07
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297

VIII. Claims Appendix

1. A method for authenticating a first user in a protected network to an application shared concurrently with a second user in an unprotected network, said method comprising the steps of:

the first user supplying a userID and a password to a first server within said protected network for authentication for said application, said application residing in a third network configured as a buffer between said protected network and said unprotected network;

said first server determining that said userID and password are authentic, and in response, said first server forwarding to said application an authentication key for said first user and a selection by said first user pertaining to said application, said password not being sent from said protected network into said third network to access said application;

said application determining that said key is authentic, and in response, said application complying with said selection by said first user; and

said second user supplying another userID and another password to said application, said application determining that said other userID and said other password are authentic, and in response, said application complying with a selection made by said second user pertaining to said application.

2. A method as set forth in claim 1 wherein said application complies with said selection made by said second user without said second user supplying an authentication key to said third network.

3. A method as set forth in claim 1 wherein said protected network and said third network are both controlled by a same entity.

4. A method as set forth in claim 1 wherein said third network is a Demilitarized Zone ("DMZ") network and acts as a security buffer for said protected network.

5. A method as set forth in claim 1 wherein said unprotected network is an Internet.

6. A method as set forth in claim 3 wherein said unprotected network is an Internet.

7. A method as set forth in claim 1 wherein said selection by said first user is a request to said application, and said selection by said second user is a request to said application.

11. A method as set forth in claim 1 wherein said application is an electronic meeting application, both said first user and said second user concurrently participate in a same meeting, and said first user selects a screen that is concurrently presented to both said first user and said second user.

12. A method as set forth in claim 11 wherein said selection by said first user is a selection of an electronic meeting in which to participate.

13. A method as set forth in claim 1 further comprising the step of said application sending to said first server said authentication key before the step of said first server forwarding to said application said authentication key.

14. A method as set forth in claim 1 wherein said authentication key is self authenticating based on whether a period during which the key is valid matches a scheduled period of use of said application, and whether an IP address of said first user is from said protected network.

16. An authentication system comprising:

an application on a first server in a first network;

a second server in a second, protected network to receive from a first user within said second network a userID and a password for authentication for said application, said second server including means for checking authentication of said first user based on said userID and password, and if said first user is authentic, forwarding to said application an authentication key for said first user and a selection by said first user pertaining to said application, said password not being sent from said protected network into said first network to access said application; and

said application including means for checking authentication of said key, and if authentic, complying with said selection by said first user; and

a workstation in a third, unprotected network for a second user, said application being shared concurrently with said first and second users, said first network configured as a buffer between said second, protected network and said third, unprotected network; and wherein

said application receives from said second user another userID and another password, and includes means for determining that said other userID and other password are authentic, and in response, complying with a selection made by said second user pertaining to said application.

17. A system as set forth in claim 16 wherein said application complies with said selection made by said second user without said second user supplying an authentication key to said first network.

18. A system as set forth in claim 16 wherein said first and second servers and said first and second networks are all controlled by a same entity.

19. A system as set forth in claim 16 wherein said first network is a Demilitarized Zone ("DMZ") network and acts as a security buffer for said protected network.

20. A system as set forth in claim 16 wherein said unprotected network is an Internet.

21. A computer program product for authenticating a first user in a protected network to an application shared simultaneously with a second user in an unprotected network, and authenticating said second user to said application, said program product comprising:

a computer readable medium;

first program instructions, for execution on a first server within said protected network, to receive from the first user a userID and a password for authentication for said application, said application residing in a third network configured as a security buffer between said protected network and said unprotected network;

second program instructions, for execution on said first server, to check authentication of said first user based on said userID and password, and if said first user is authentic, to forward to said application an authentication key for said first user and a selection by said first user pertaining to said application, said password not being sent from said protected network into said third network to access said application;

third program instructions in said application to check authentication of said key, and if authentic, comply with said selection by said first user;

fourth program instructions in said application to receive from said second user another userID and another password, determine if said other userID and other password are authentic, and if so, instruct said application to comply with a selection made by said second user pertaining to said application; and wherein

said first, second, third and fourth program instructions are recorded on said medium in functional form.

22. A computer program product as set forth in claim 21 wherein said application complies with said selection made by said second user without said second user supplying an authentication key to said third network.

23. A method for authenticating a first user of a first computer in a protected network to a second computer executing an application, a second user of a third computer in an unprotected network and said first user of said first computer concurrently sharing said application, said second computer residing in a third network configured as a buffer between said protected network and said unprotected network; said method comprising the steps of:

the first computer supplying a userID and a password of the first user to a fourth computer in said protected network for authentication for said application;

said fourth computer determining that said userID and password are authentic, and in response, forwarding to said second computer an authentication key for said first user, said password not being sent from said protected network into said third network to access said application;

said second computer determining that said key is authentic, and in response, complying with a selection by said first user pertaining to said application; and

said third computer supplying another userID and another password of said second user to said second computer, said second computer determining that said other userID and said other password are authentic, and in response, said application complying with a selection made by said second user pertaining to said application.

24. A method as set forth in claim 23 wherein said application complies with said selection made by said second user without said second user or said third computer supplying an authentication key to said second computer or said third network.

25. A method as set forth in claim 23 wherein said protected network and said third network are both controlled by a same entity.

26. A method as set forth in claim 23 wherein said third network acts as a security buffer for said protected network.

IX. Evidence Appendix

There is no evidence relied upon in this appeal, and therefore, no copies of evidence.

X. Related Proceedings Appendix

There are no related proceedings, and therefore, no copies of decisions rendered by a court or the Board.